FIG.1

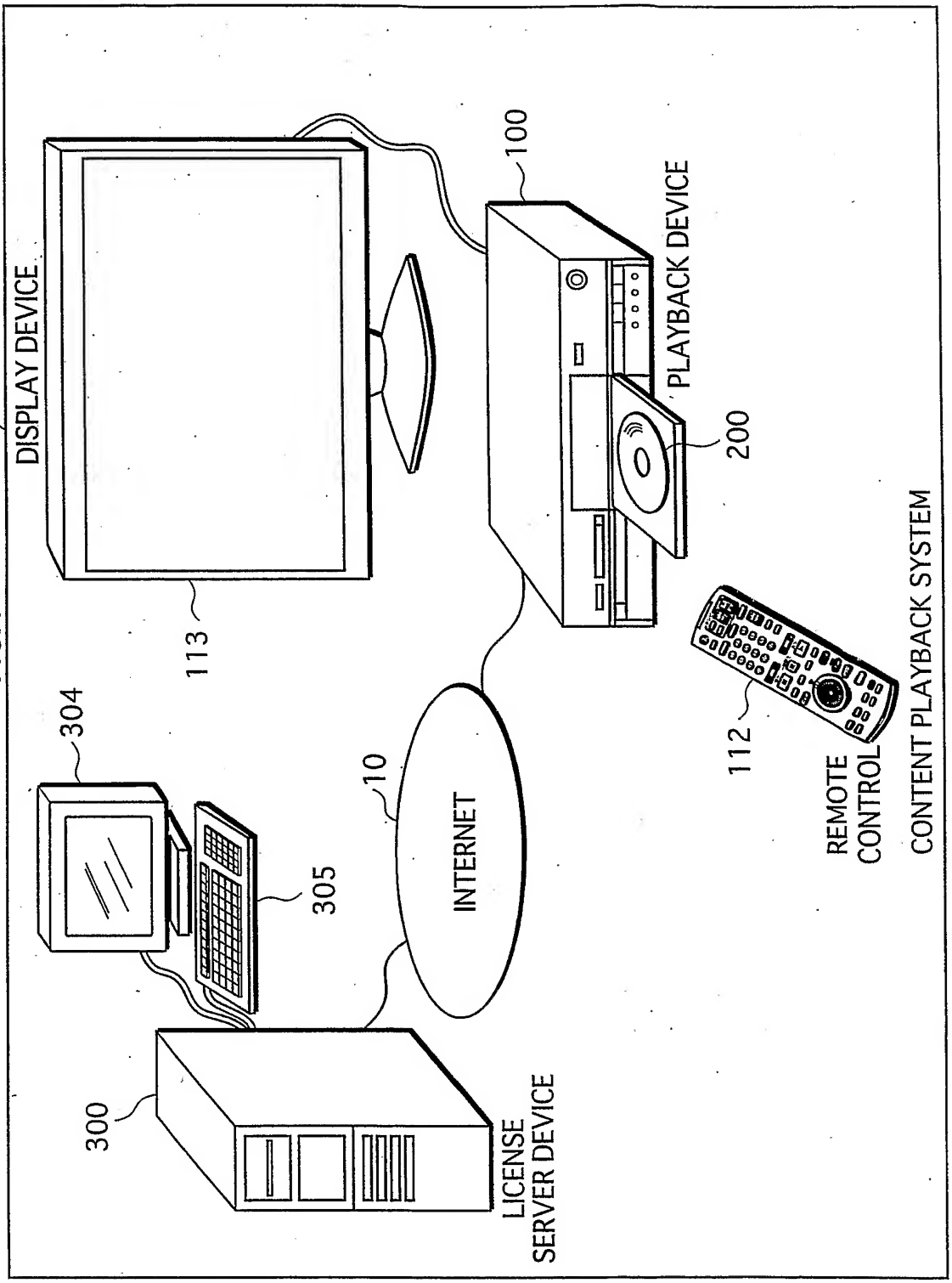

CONTENT PLAYBACK SYSTEM
1
DISPLAY DEVICE
113
100
PLAYBACK DEVICE
200
112
REMOTE CONTROL
10
INTERNET
304
305
300
LICENSE SERVER DEVICE

FIG.2

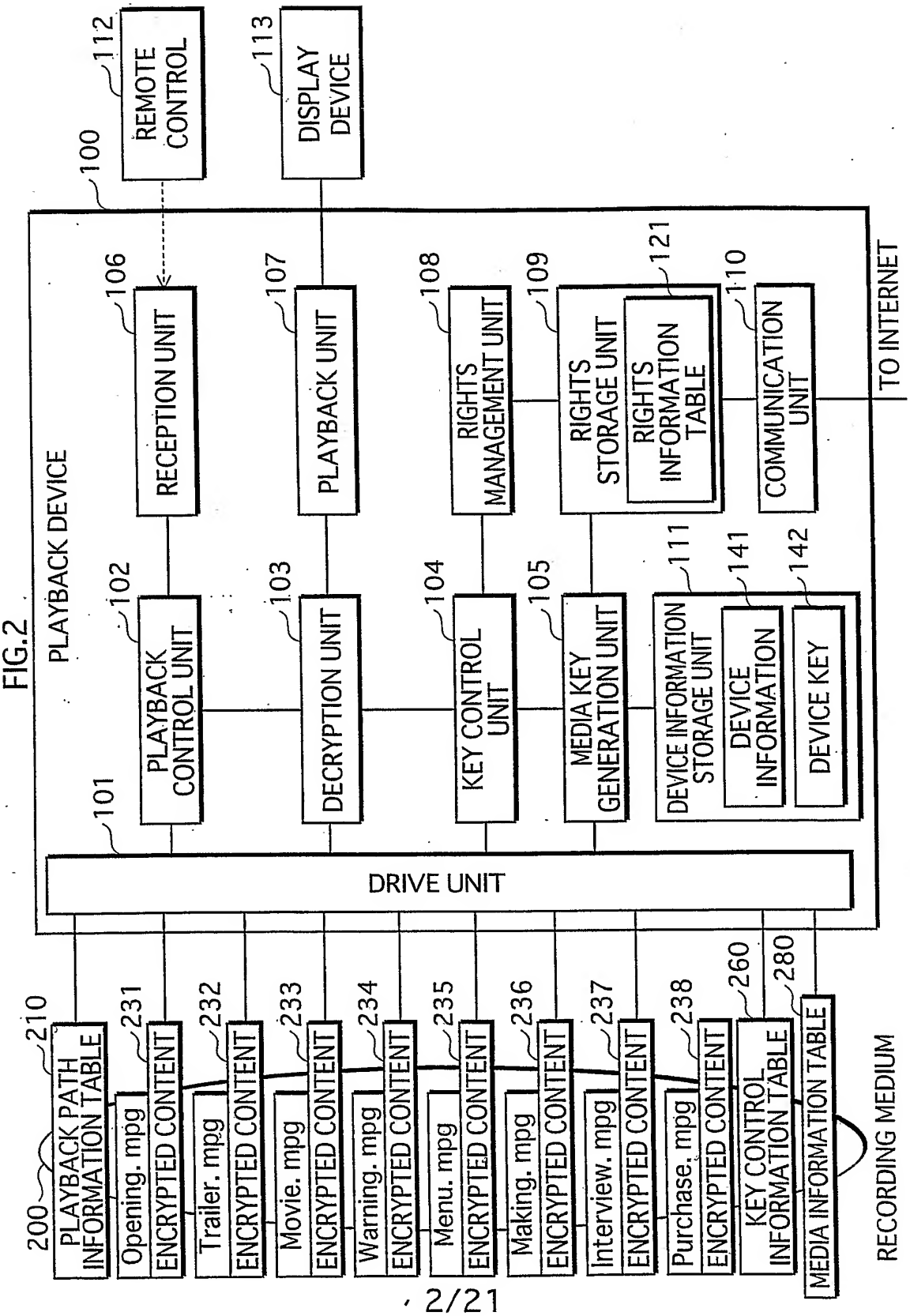

PLAYBACK DEVICE
100
REMOTE CONTROL
112
DISPLAY DEVICE
113
RECEPTION UNIT
106
PLAYBACK UNIT
107
RIGHTS MANAGEMENT UNIT
108
RIGHTS STORAGE UNIT
109
RIGHTS INFORMATION TABLE
121
COMMUNICATION UNIT
110
TO INTERNET
PLAYBACK CONTROL UNIT
102
DECRYPTION UNIT
103
KEY CONTROL UNIT
104
MEDIA KEY GENERATION UNIT
105
DEVICE INFORMATION STORAGE UNIT
111
DEVICE INFORMATION
141
DEVICE KEY
142
101
DRIVE UNIT
200
PLAYBACK PATH INFORMATION TABLE
210
Opening. mpg
ENCRYPTED CONTENT
231
Trailer. mpg
ENCRYPTED CONTENT
232
Movie. mpg
ENCRYPTED CONTENT
233
Warning. mpg
ENCRYPTED CONTENT
234
Menu. mpg
ENCRYPTED CONTENT
235
Making. mpg
ENCRYPTED CONTENT
236
Interview. mpg
ENCRYPTED CONTENT
237
Purchase. mpg
ENCRYPTED CONTENT
238
KEY CONTROL INFORMATION TABLE
260
MEDIA INFORMATION TABLE
280
RECORDING MEDIUM

FIG.3

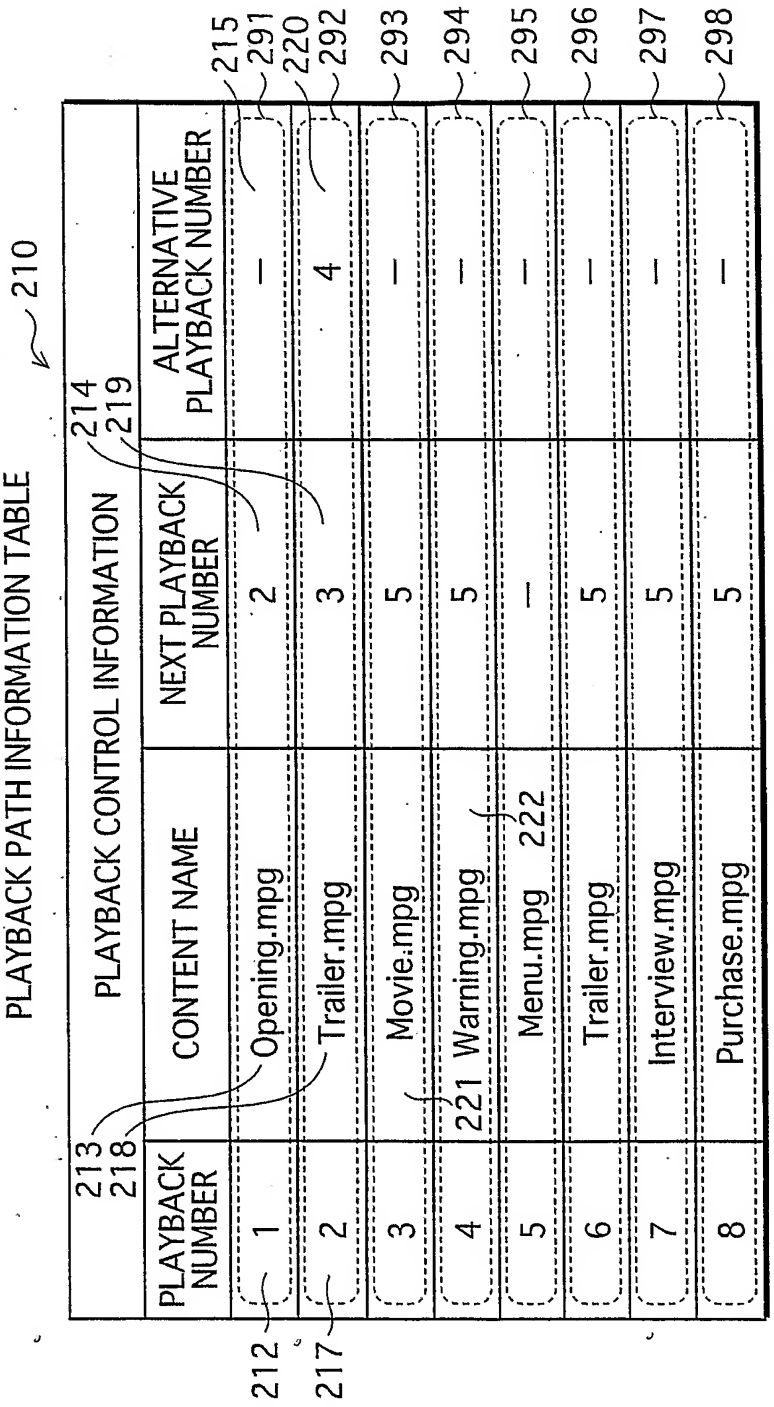

PLAYBACK PATH INFORMATION TABLE
210
PLAYBACK CONTROL INFORMATION
213
218
214
219
215
PLAYBACK NUMBER
CONTENT NAME
NEXT PLAYBACK NUMBER
ALTERNATIVE PLAYBACK NUMBER
1
Opening.mpg
2
—
291
2
Trailer.mpg
3
4
220
292
3
Movie.mpg
5
—
293
4
Warning.mpg
221
5
—
294
5
Menu.mpg
222
—
—
295
6
Trailer.mpg
5
—
296
7
Interview.mpg
5
—
297
8
Purchase.mpg
5
—
298
212
217

FIG.4

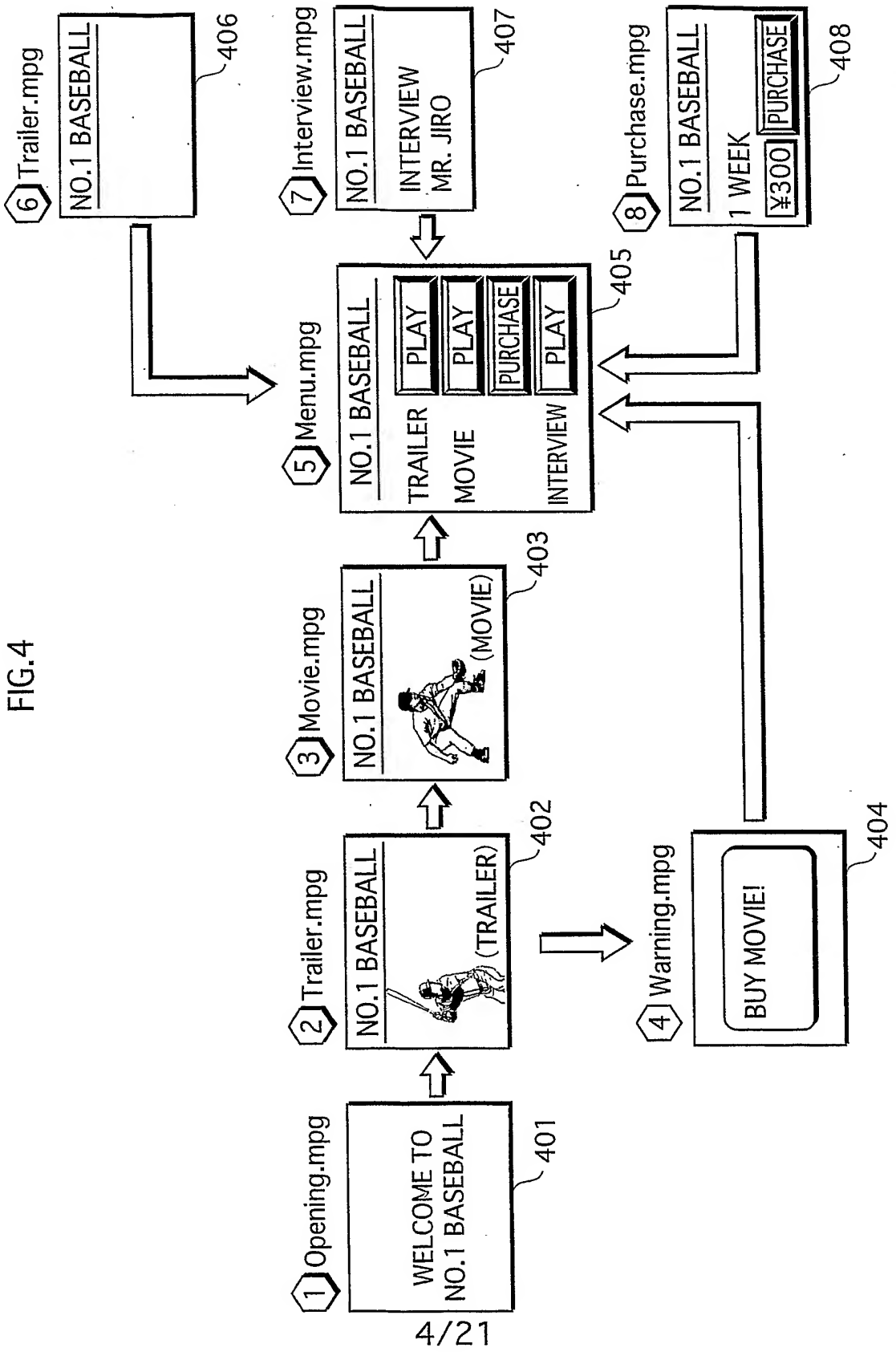

1 Opening.mpg
WELCOME TO NO.1 BASEBALL
401
2 Trailer.mpg
NO.1 BASEBALL
(TRAILER)
402
3 Movie.mpg
NO.1 BASEBALL
(MOVIE)
403
4 Warning.mpg
BUY MOVIE!
404
5 Menu.mpg
NO.1 BASEBALL
TRAILER
MOVIE
INTERVIEW
PLAY
PLAY
PURCHASE
PLAY
405
6 Trailer.mpg
NO.1 BASEBALL
406
7 Interview.mpg
NO.1 BASEBALL
INTERVIEW
MR. JIRO
407
8 Purchase.mpg
NO.1 BASEBALL
1 WEEK
¥300
PURCHASE
408

FIG.5

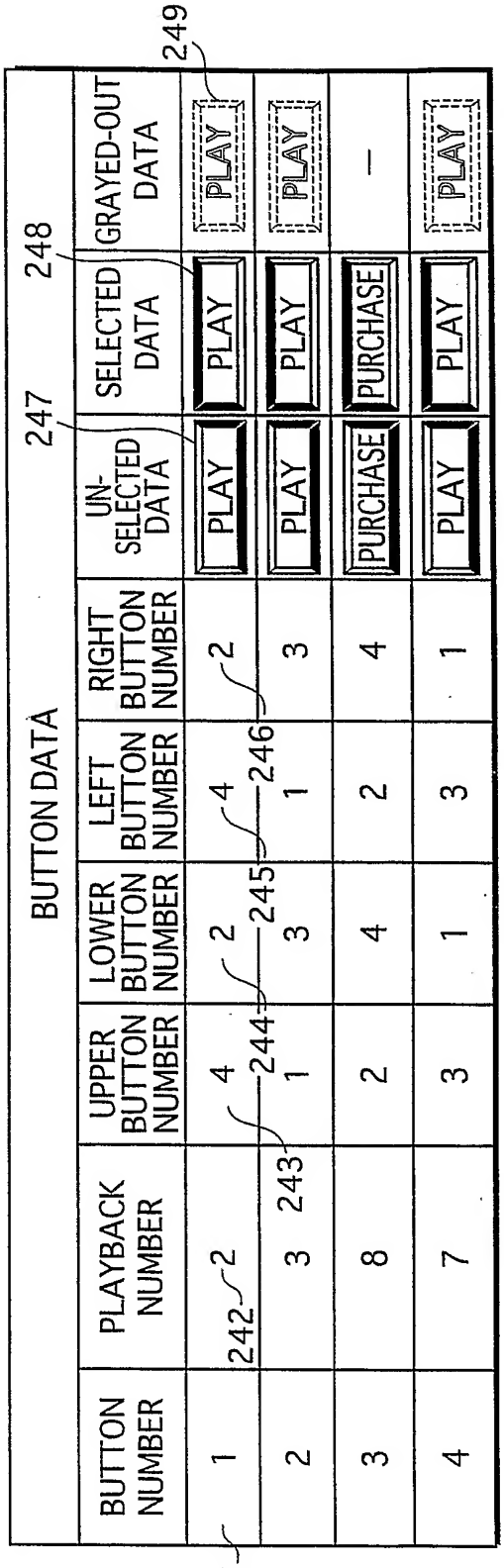

BUTTON DATA TABLE
240
BUTTON DATA
247
248
249
241
BUTTON NUMBER
PLAYBACK NUMBER
UPPER BUTTON NUMBER
LOWER BUTTON NUMBER
LEFT BUTTON NUMBER
RIGHT BUTTON NUMBER
UN-SELECTED DATA
SELECTED DATA
GRAYED-OUT DATA
1
2
3
4
242
243
244
245
246
PLAY
PURCHASE
—

FIG.6

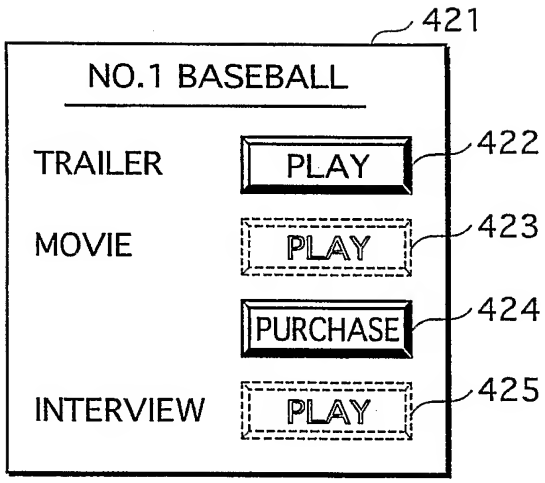

421
NO.1 BASEBALL
TRAILER
PLAY
422
MOVIE
PLAY
423
PURCHASE
424
INTERVIEW
PLAY
425

FIG.7

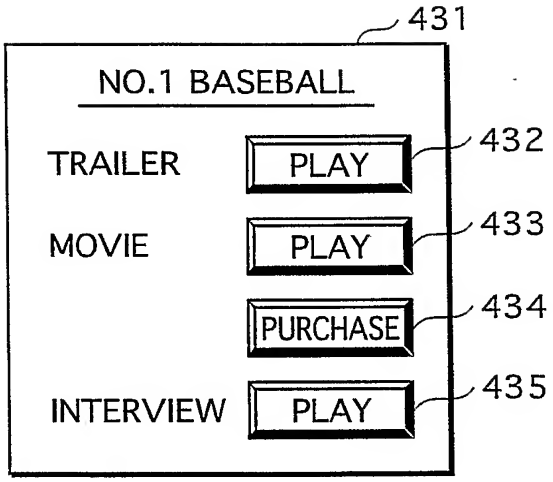

431
NO.1 BASEBALL
TRAILER
PLAY
432
MOVIE
PLAY
433
PURCHASE
434
INTERVIEW
PLAY
435

FIG.8

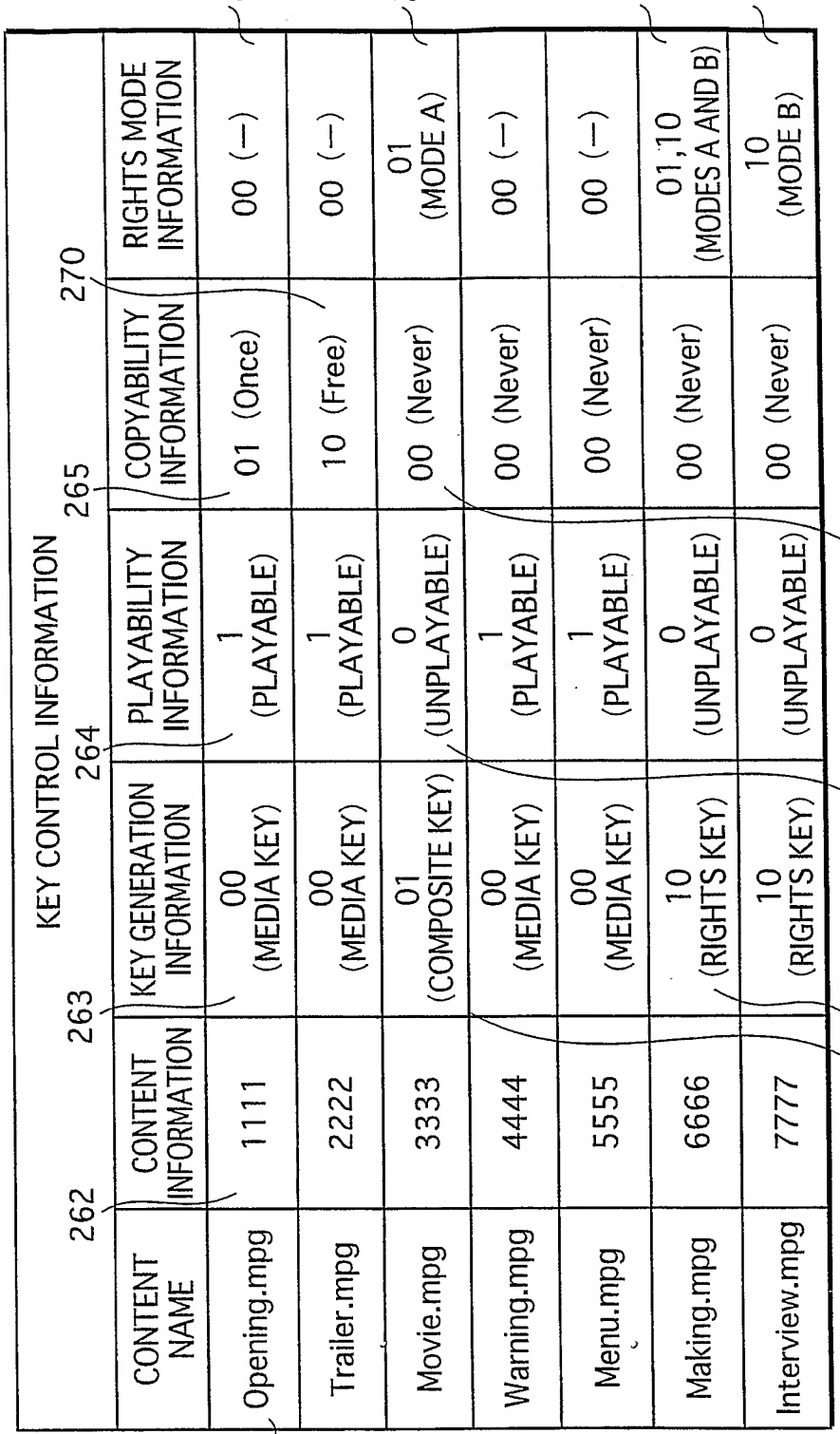

KEY CONTROL INFORMATION TABLE
260
KEY CONTROL INFORMATION
262
263
264
265
270
266
272
273
274
271
269
268
267
261
CONTENT NAME
CONTENT INFORMATION
KEY GENERATION INFORMATION
PLAYABILITY INFORMATION
COPYABILITY INFORMATION
RIGHTS MODE INFORMATION
Opening.mpg
1111
00 (MEDIA KEY)
1 (PLAYABLE)
01 (Once)
00 (—)
Trailer.mpg
2222
00 (MEDIA KEY)
1 (PLAYABLE)
10 (Free)
00 (—)
Movie.mpg
3333
01 (COMPOSITE KEY)
0 (UNPLAYABLE)
00 (Never)
01 (MODE A)
Warning.mpg
4444
00 (MEDIA KEY)
1 (PLAYABLE)
00 (Never)
00 (—)
Menu.mpg
5555
00 (MEDIA KEY)
1 (PLAYABLE)
00 (Never)
00 (—)
Making.mpg
6666
10 (RIGHTS KEY)
0 (UNPLAYABLE)
00 (Never)
01,10 (MODES A AND B)
Interview.mpg
7777
10 (RIGHTS KEY)
0 (UNPLAYABLE)
00 (Never)
10 (MODE B)

FIG. 9

MEDIA INFORMATION TABLE

280

MEDIA INFORMATION	
DEVICE INFORMATION	ENCRYPTED MEDIA KEY
0001	qwerty
0002	asdfgh
0004	zxcvbn
0005	uiop@[
0006	jkl;:]
0007	m,./¥¥
⋮	⋮

281

282

FIG.10

RIGHTS INFORMATION TABLE

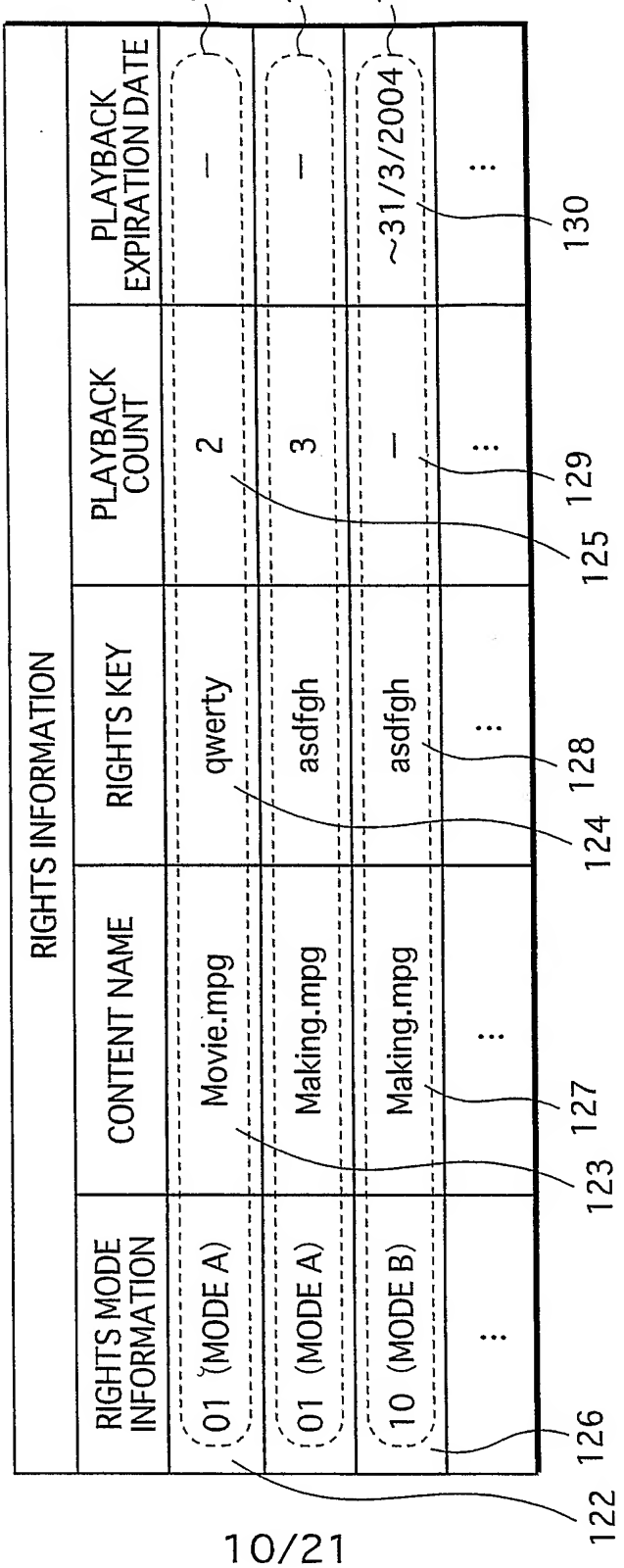


FIG.11

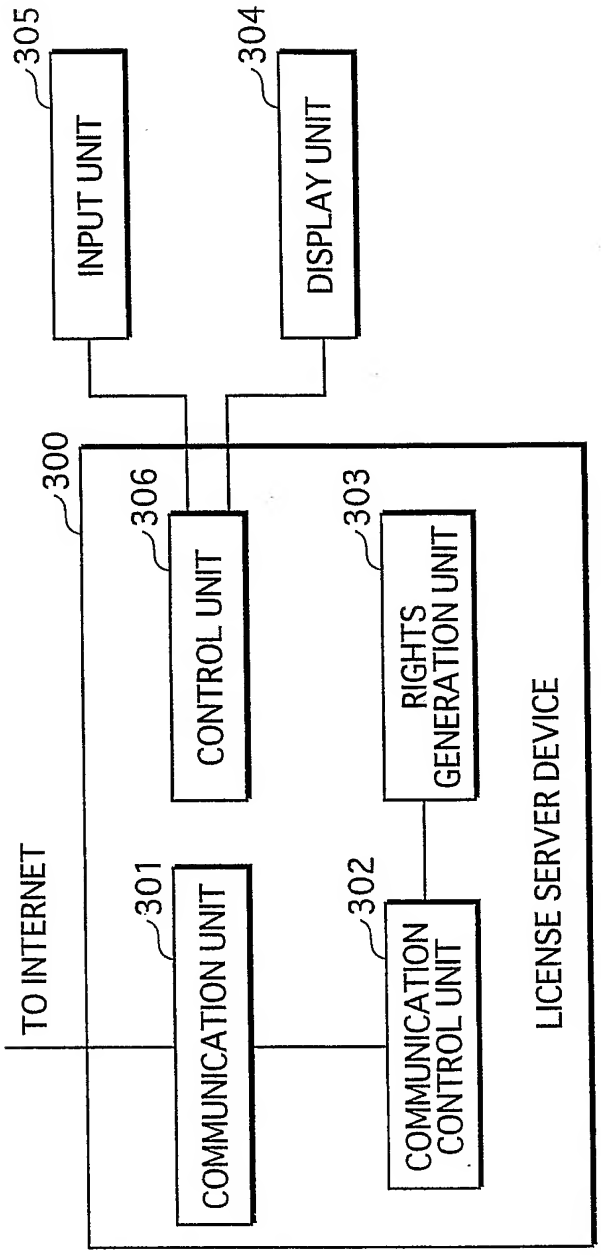

305
INPUT UNIT
304
DISPLAY UNIT
300
306
CONTROL UNIT
303
RIGHTS GENERATION UNIT
TO INTERNET
301
COMMUNICATION UNIT
302
COMMUNICATION CONTROL UNIT
LICENSE SERVER DEVICE

FIG.12

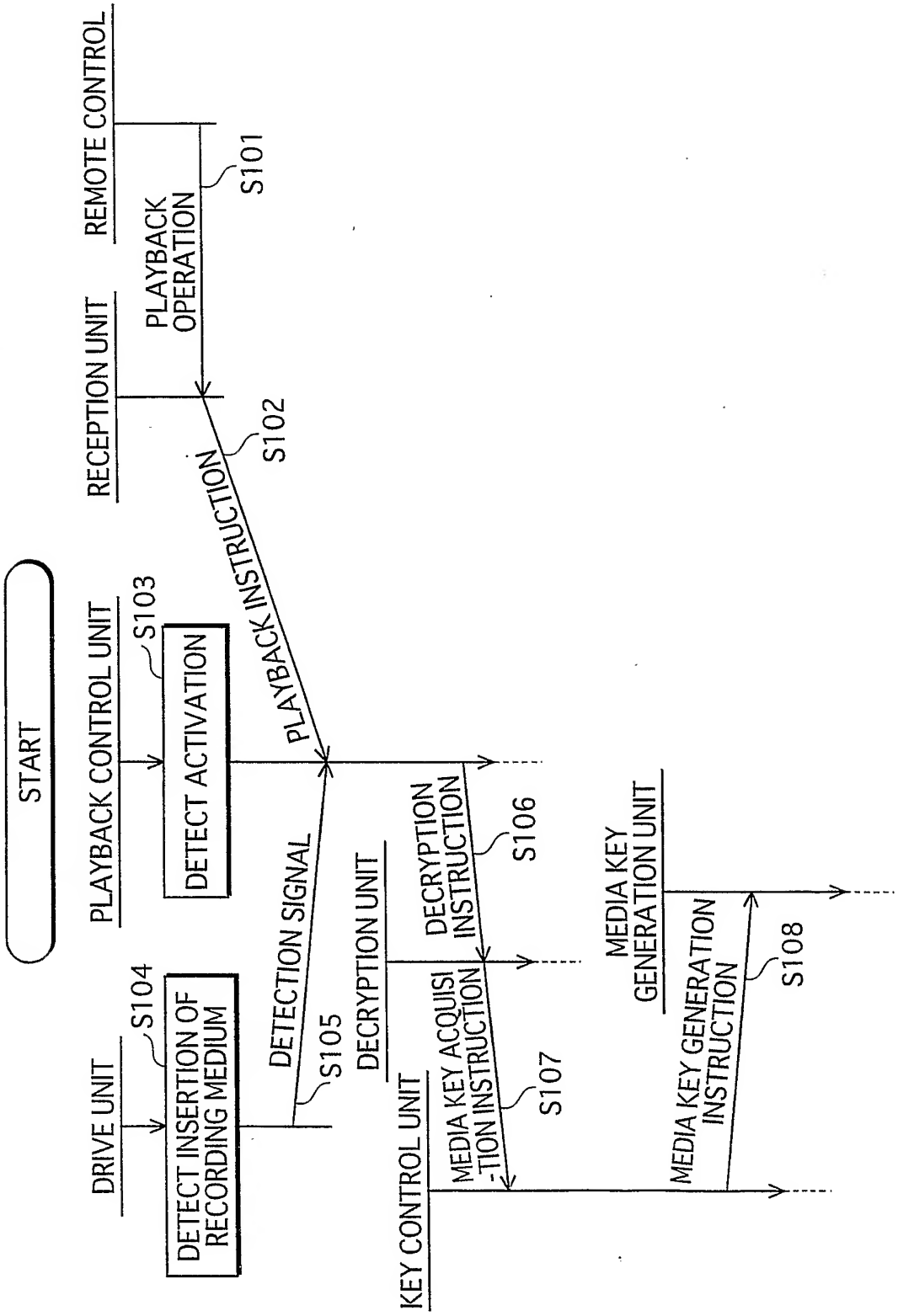

START
REMOTE CONTROL
RECEPTION UNIT
PLAYBACK OPERATION
S101
PLAYBACK INSTRUCTION
S102
PLAYBACK CONTROL UNIT
S103
DETECT ACTIVATION
DRIVE UNIT
S104
DETECT INSERTION OF RECORDING MEDIUM
DETECTION SIGNAL
S105
DECRYPTION UNIT
DECRYPTION INSTRUCTION
S106
KEY CONTROL UNIT
MEDIA KEY ACQUISI -TION INSTRUCTION
S107
MEDIA KEY GENERATION UNIT
MEDIA KEY GENERATION INSTRUCTION
S108

FIG. 13

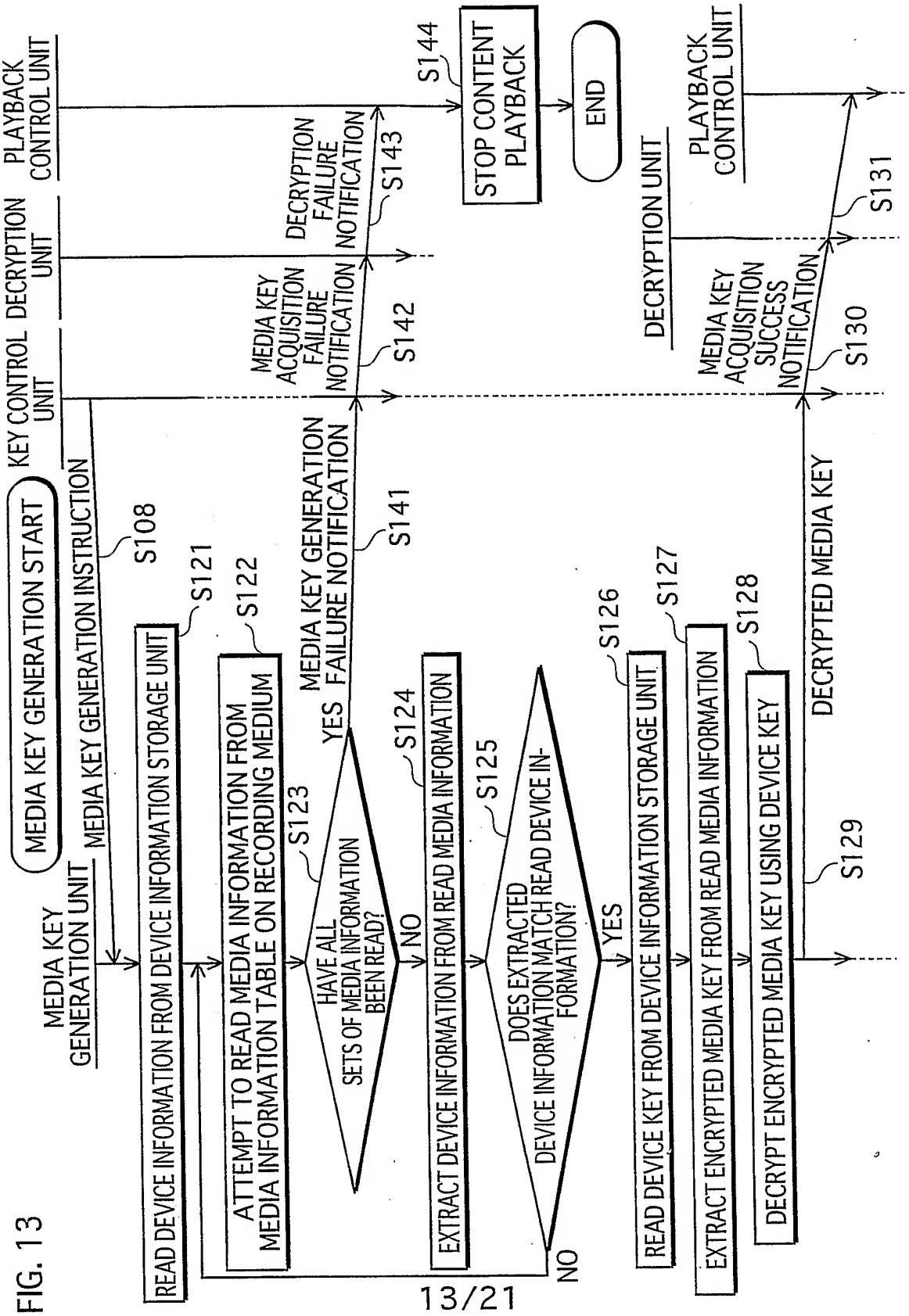

MEDIA KEY GENERATION START
MEDIA KEY GENERATION UNIT
KEY CONTROL UNIT
DECRYPTION UNIT
PLAYBACK CONTROL UNIT
MEDIA KEY GENERATION INSTRUCTION
S108
READ DEVICE INFORMATION FROM DEVICE INFORMATION STORAGE UNIT
S121
ATTEMPT TO READ MEDIA INFORMATION FROM MEDIA INFORMATION TABLE ON RECORDING MEDIUM
S122
HAVE ALL SETS OF MEDIA INFORMATION BEEN READ?
S123
YES
MEDIA KEY GENERATION FAILURE NOTIFICATION
S141
NO
EXTRACT DEVICE INFORMATION FROM READ MEDIA INFORMATION
S124
DOES EXTRACTED DEVICE INFORMATION MATCH READ DEVICE INFORMATION?
S125
NO
YES
READ DEVICE KEY FROM DEVICE INFORMATION STORAGE UNIT
S126
EXTRACT ENCRYPTED MEDIA KEY FROM READ MEDIA INFORMATION
S127
DECRYPT ENCRYPTED MEDIA KEY USING DEVICE KEY
S128
DECRYPTED MEDIA KEY
S129
MEDIA KEY ACQUISITION FAILURE NOTIFICATION
S142
DECRYPTION FAILURE NOTIFICATION
S143
STOP CONTENT PLAYBACK
S144
END
MEDIA KEY ACQUISITION SUCCESS NOTIFICATION
S130
S131

FIG. 14

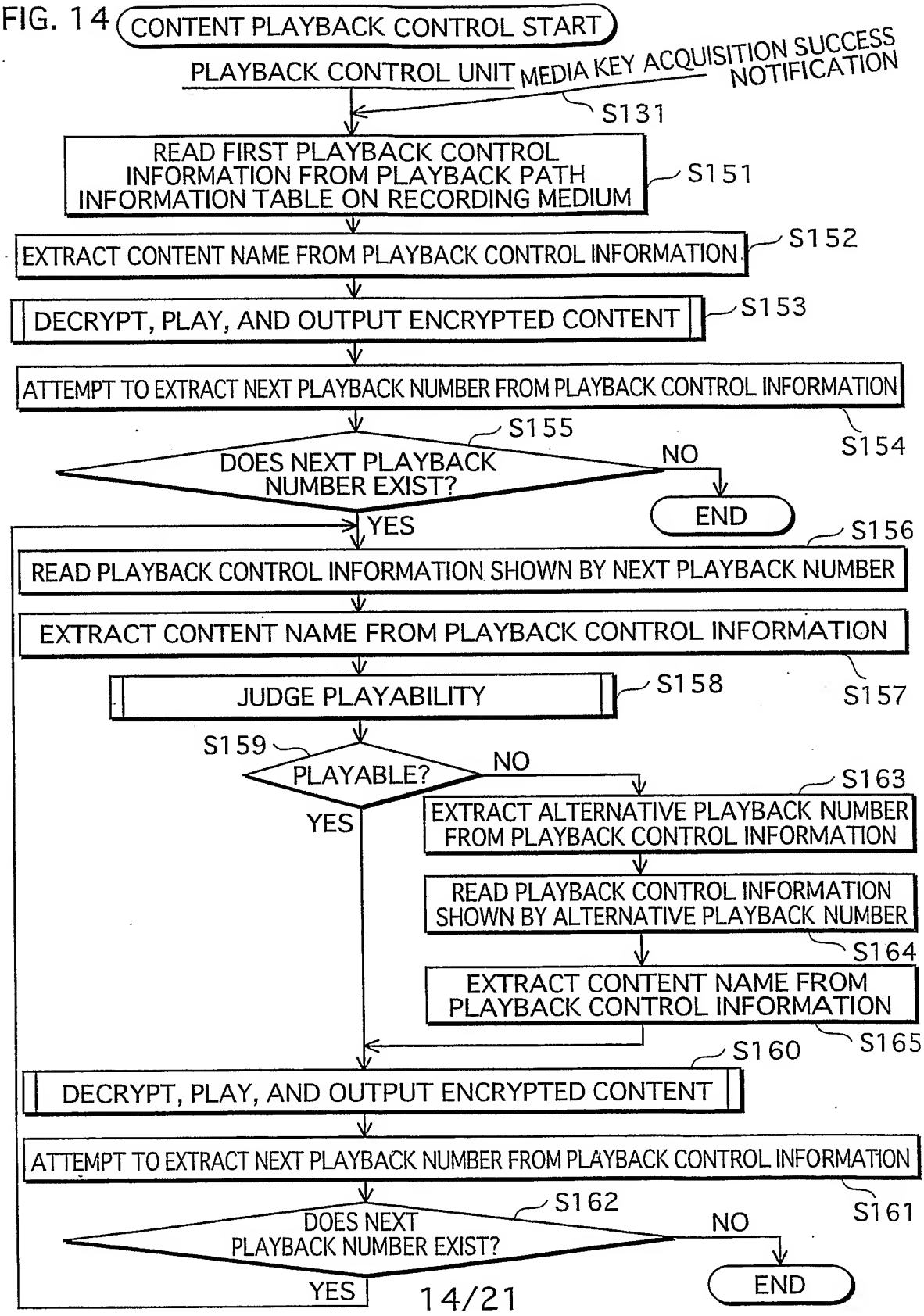

CONTENT PLAYBACK CONTROL START
PLAYBACK CONTROL UNIT
MEDIA KEY ACQUISITION SUCCESS NOTIFICATION
S131
READ FIRST PLAYBACK CONTROL INFORMATION FROM PLAYBACK PATH INFORMATION TABLE ON RECORDING MEDIUM
S151
EXTRACT CONTENT NAME FROM PLAYBACK CONTROL INFORMATION
S152
DECRYPT, PLAY, AND OUTPUT ENCRYPTED CONTENT
S153
ATTEMPT TO EXTRACT NEXT PLAYBACK NUMBER FROM PLAYBACK CONTROL INFORMATION
S154
S155
DOES NEXT PLAYBACK NUMBER EXIST?
NO
END
YES
S156
READ PLAYBACK CONTROL INFORMATION SHOWN BY NEXT PLAYBACK NUMBER
EXTRACT CONTENT NAME FROM PLAYBACK CONTROL INFORMATION
S157
JUDGE PLAYABILITY
S158
S159
PLAYABLE?
NO
S163
EXTRACT ALTERNATIVE PLAYBACK NUMBER FROM PLAYBACK CONTROL INFORMATION
YES
READ PLAYBACK CONTROL INFORMATION SHOWN BY ALTERNATIVE PLAYBACK NUMBER
S164
EXTRACT CONTENT NAME FROM PLAYBACK CONTROL INFORMATION
S165
S160
DECRYPT, PLAY, AND OUTPUT ENCRYPTED CONTENT
ATTEMPT TO EXTRACT NEXT PLAYBACK NUMBER FROM PLAYBACK CONTROL INFORMATION
S161
S162
DOES NEXT PLAYBACK NUMBER EXIST?
NO
END
YES

FIG.15

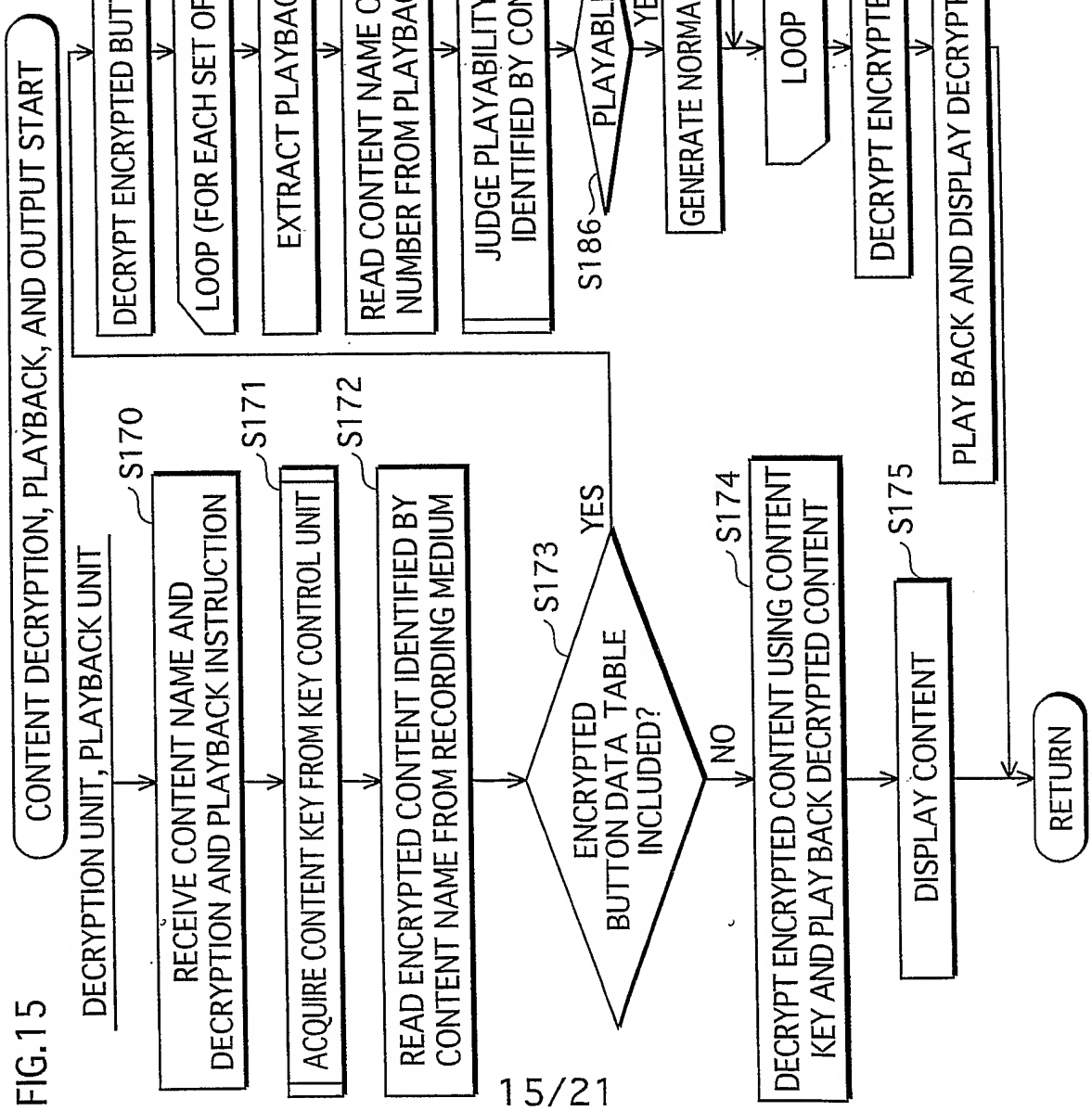

CONTENT DECRYPTION, PLAYBACK, AND OUTPUT START
DECRYPTION UNIT, PLAYBACK UNIT
S170
RECEIVE CONTENT NAME AND DECRYPTION AND PLAYBACK INSTRUCTION
S171
ACQUIRE CONTENT KEY FROM KEY CONTROL UNIT
S172
READ ENCRYPTED CONTENT IDENTIFIED BY CONTENT NAME FROM RECORDING MEDIUM
S173
ENCRYPTED BUTTON DATA TABLE INCLUDED?
YES
NO
S174
DECRYPT ENCRYPTED CONTENT USING CONTENT KEY AND PLAY BACK DECRYPTED CONTENT
S175
DISPLAY CONTENT
RETURN
S181
DECRYPT ENCRYPTED BUTTON DATA TABLE
S182
LOOP (FOR EACH SET OF BUTTON DATA)
S183
EXTRACT PLAYBACK NUMBER
S184
READ CONTENT NAME CORRESPONDING TO PLAYBACK NUMBER FROM PLAYBACK PATH INFORMATION TABLE
S185
JUDGE PLAYABILITY OF CONTENT IDENTIFIED BY CONTENT NAME
S186
PLAYABLE?
NO
S188
GENERATE GRAYED-OUT BUTTON
YES
S187
GENERATE NORMAL BUTTON
S189
LOOP
S190
DECRYPT ENCRYPTED CONTENT
S191
PLAY BACK AND DISPLAY DECRYPTED CONTENT AND BUTTON

FIG.16

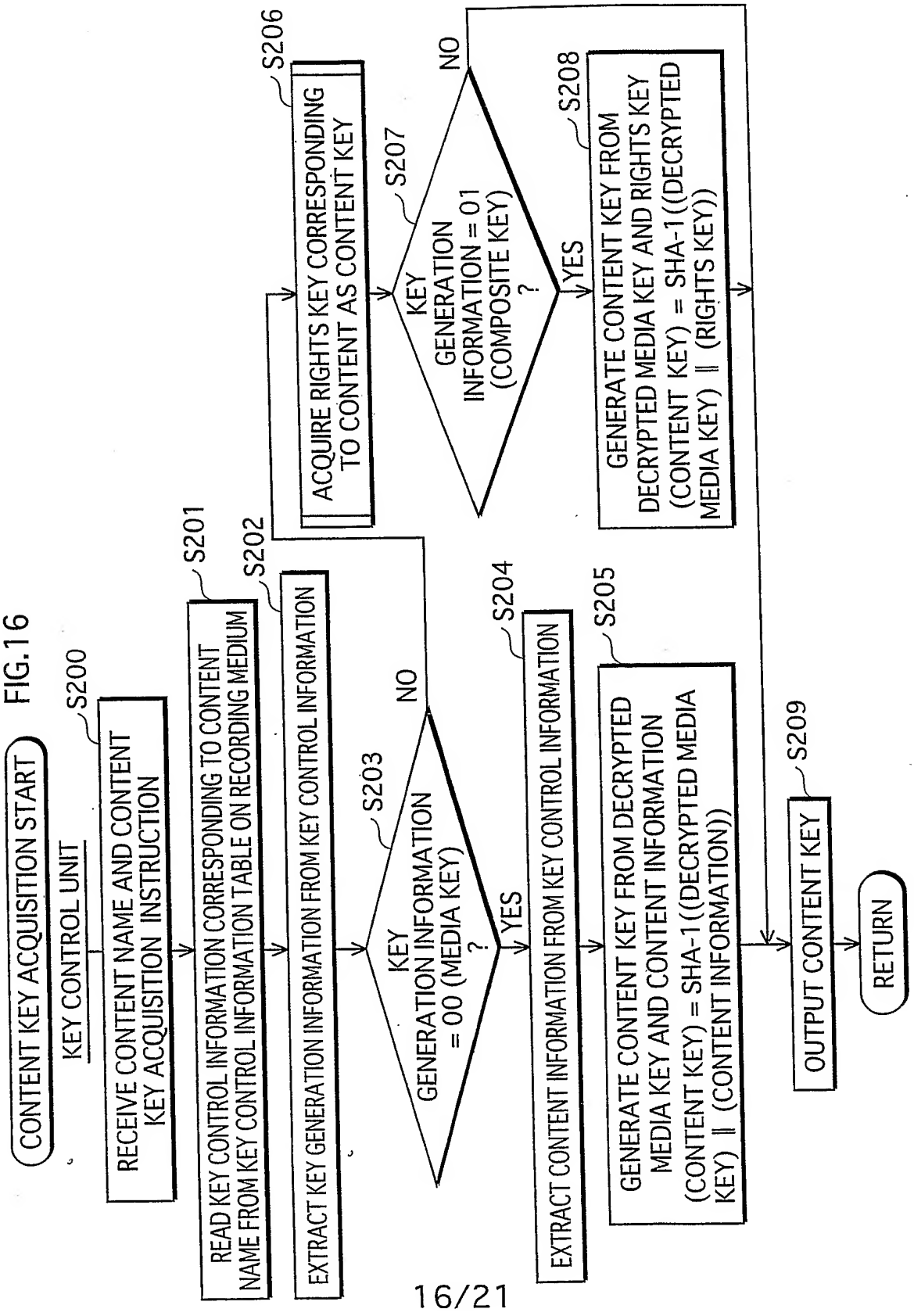

CONTENT KEY ACQUISITION START
KEY CONTROL UNIT
S200
RECEIVE CONTENT NAME AND CONTENT KEY ACQUISITION INSTRUCTION
S201
READ KEY CONTROL INFORMATION CORRESPONDING TO CONTENT NAME FROM KEY CONTROL INFORMATION TABLE ON RECORDING MEDIUM
S202
EXTRACT KEY GENERATION INFORMATION FROM KEY CONTROL INFORMATION
S203
KEY GENERATION INFORMATION = 00 (MEDIA KEY) ?
NO
YES
S204
EXTRACT CONTENT INFORMATION FROM KEY CONTROL INFORMATION
S205
GENERATE CONTENT KEY FROM DECRYPTED MEDIA KEY AND CONTENT INFORMATION (CONTENT KEY) = SHA-1((DECRYPTED MEDIA KEY) || (CONTENT INFORMATION))
S206
ACQUIRE RIGHTS KEY CORRESPONDING TO CONTENT AS CONTENT KEY
S207
KEY GENERATION INFORMATION = 01 (COMPOSITE KEY) ?
NO
YES
S208
GENERATE CONTENT KEY FROM DECRYPTED MEDIA KEY AND RIGHTS KEY (CONTENT KEY) = SHA-1((DECRYPTED MEDIA KEY) || (RIGHTS KEY))
S209
OUTPUT CONTENT KEY
RETURN

FIG.17

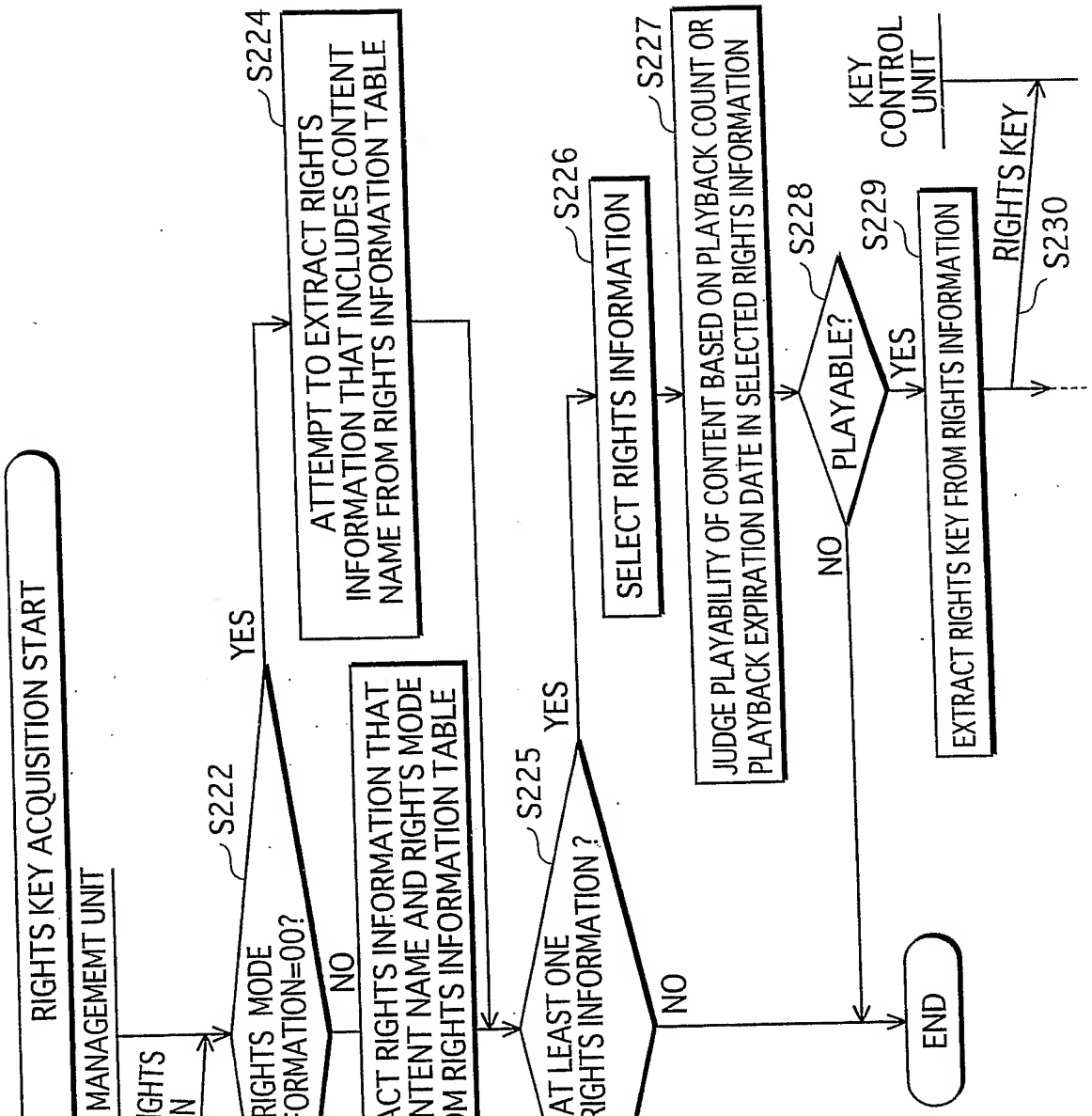

RIGHTS KEY ACQUISITION START
KEY CONTROL UNIT
RIGHTS MANAGEMEMT UNIT
CONTENT NAME AND RIGHTS MODE INFORMATION
S221
S222
RIGHTS MODE INFORMATION=00?
YES
NO
S223
ATTEMPT TO EXTRACT RIGHTS INFORMATION THAT INCLUDES BOTH CONTENT NAME AND RIGHTS MODE INFORMATION, FROM RIGHTS INFORMATION TABLE
S224
ATTEMPT TO EXTRACT RIGHTS INFORMATION THAT INCLUDES CONTENT NAME FROM RIGHTS INFORMATION TABLE
S225
AT LEAST ONE SET OF RIGHTS INFORMATION ?
YES
NO
S226
SELECT RIGHTS INFORMATION
S227
JUDGE PLAYABILITY OF CONTENT BASED ON PLAYBACK COUNT OR PLAYBACK EXPIRATION DATE IN SELECTED RIGHTS INFORMATION
S228
PLAYABLE?
NO
YES
S229
KEY CONTROL UNIT
EXTRACT RIGHTS KEY FROM RIGHTS INFORMATION
RIGHTS KEY
S230
END

FIG.18

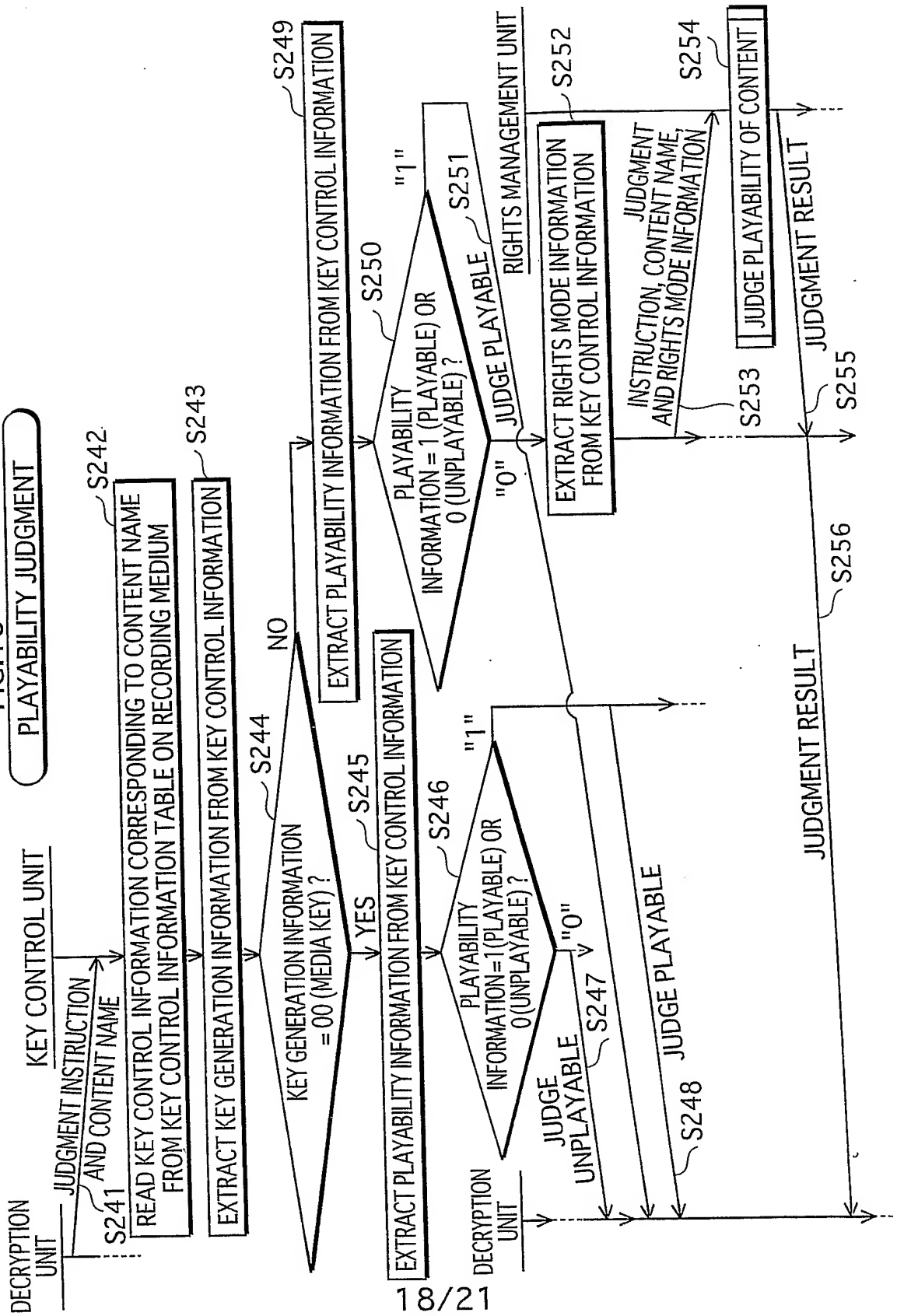

PLAYABILITY JUDGMENT
KEY CONTROL UNIT
DECRYPTION UNIT
JUDGMENT INSTRUCTION AND CONTENT NAME
S241
READ KEY CONTROL INFORMATION CORRESPONDING TO CONTENT NAME FROM KEY CONTROL INFORMATION TABLE ON RECORDING MEDIUM
S242
EXTRACT KEY GENERATION INFORMATION FROM KEY CONTROL INFORMATION
S243
KEY GENERATION INFORMATION = 00 (MEDIA KEY) ?
S244
NO
YES
EXTRACT PLAYABILITY INFORMATION FROM KEY CONTROL INFORMATION
S245
EXTRACT PLAYABILITY INFORMATION FROM KEY CONTROL INFORMATION
S246
PLAYABILITY INFORMATION=1(PLAYABLE) OR 0(UNPLAYABLE) ?
"1"
"0"
JUDGE UNPLAYABLE
S247
JUDGE PLAYABLE
S248
DECRYPTION UNIT
S249
EXTRACT PLAYABILITY INFORMATION FROM KEY CONTROL INFORMATION
S250
PLAYABILITY INFORMATION = 1 (PLAYABLE) OR 0 (UNPLAYABLE) ?
"1"
"0"
S251
JUDGE PLAYABLE
RIGHTS MANAGEMENT UNIT
S252
EXTRACT RIGHTS MODE INFORMATION FROM KEY CONTROL INFORMATION
JUDGMENT INSTRUCTION, CONTENT NAME, AND RIGHTS MODE INFORMATION
S253
S254
JUDGE PLAYABILITY OF CONTENT
JUDGMENT RESULT
S255
JUDGMENT RESULT
S256

FIG.19

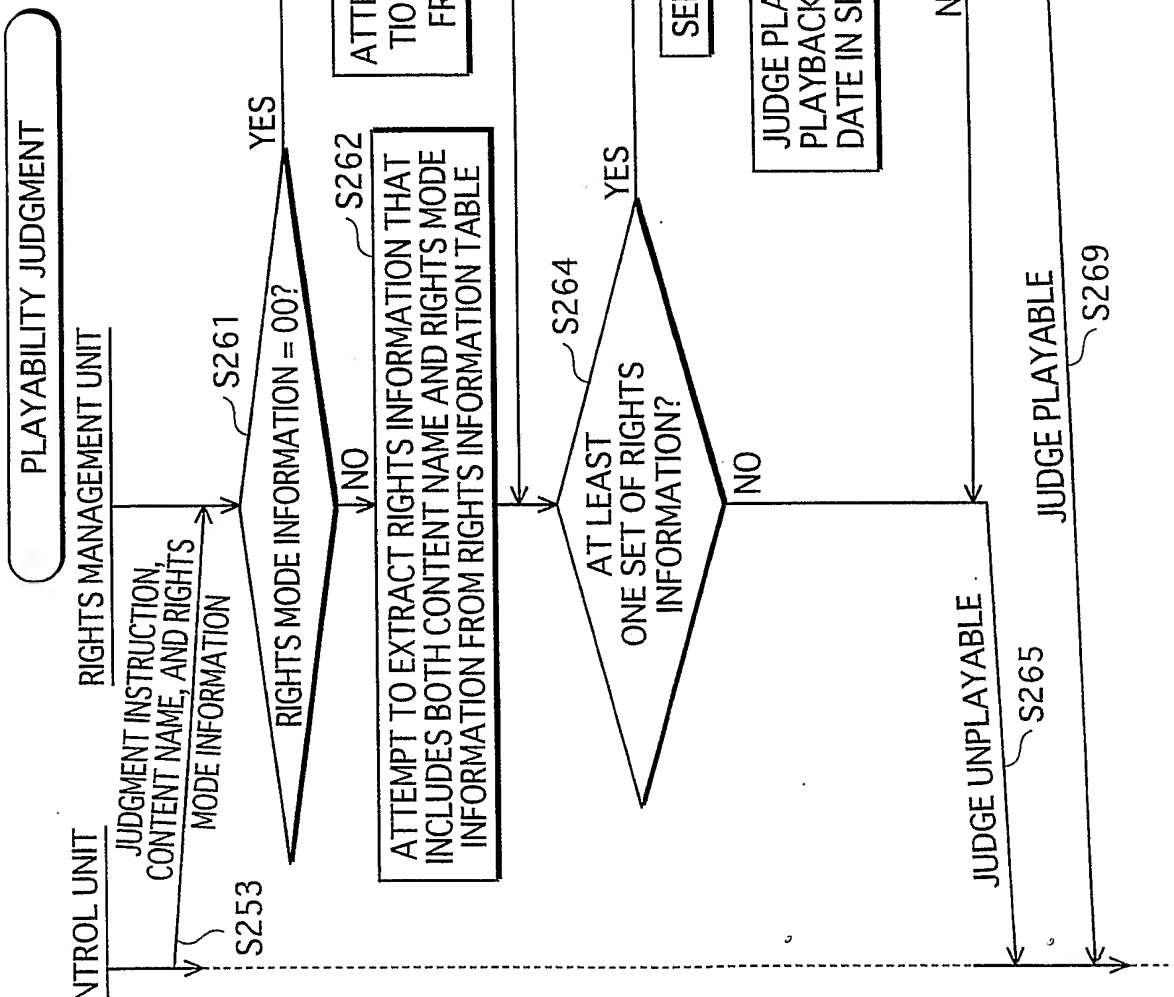

PLAYABILITY JUDGMENT
KEY CONTROL UNIT
RIGHTS MANAGEMENT UNIT
JUDGMENT INSTRUCTION, CONTENT NAME, AND RIGHTS MODE INFORMATION
S253
S261
RIGHTS MODE INFORMATION = 00?
YES
NO
S262
ATTEMPT TO EXTRACT RIGHTS INFORMATION THAT INCLUDES BOTH CONTENT NAME AND RIGHTS MODE INFORMATION FROM RIGHTS INFORMATION TABLE
S263
ATTEMPT TO EXTRACT RIGHTS INFORMATION THAT INCLUDES CONTENT NAME FROM RIGHTS INFORMATION TABLE
S264
AT LEAST ONE SET OF RIGHTS INFORMATION?
YES
NO
S266
SELECT RIGHTS INFORMATION
S267
JUDGE PLAYABILITY OF CONTENT BASED ON PLAYBACK COUNT OR PLAYBACK EXPIRATION DATE IN SELECTED RIGHTS INFORMATION
S268
PLAYABLE?
YES
NO
S265
JUDGE UNPLAYABLE
S269
JUDGE PLAYABLE

FIG. 20

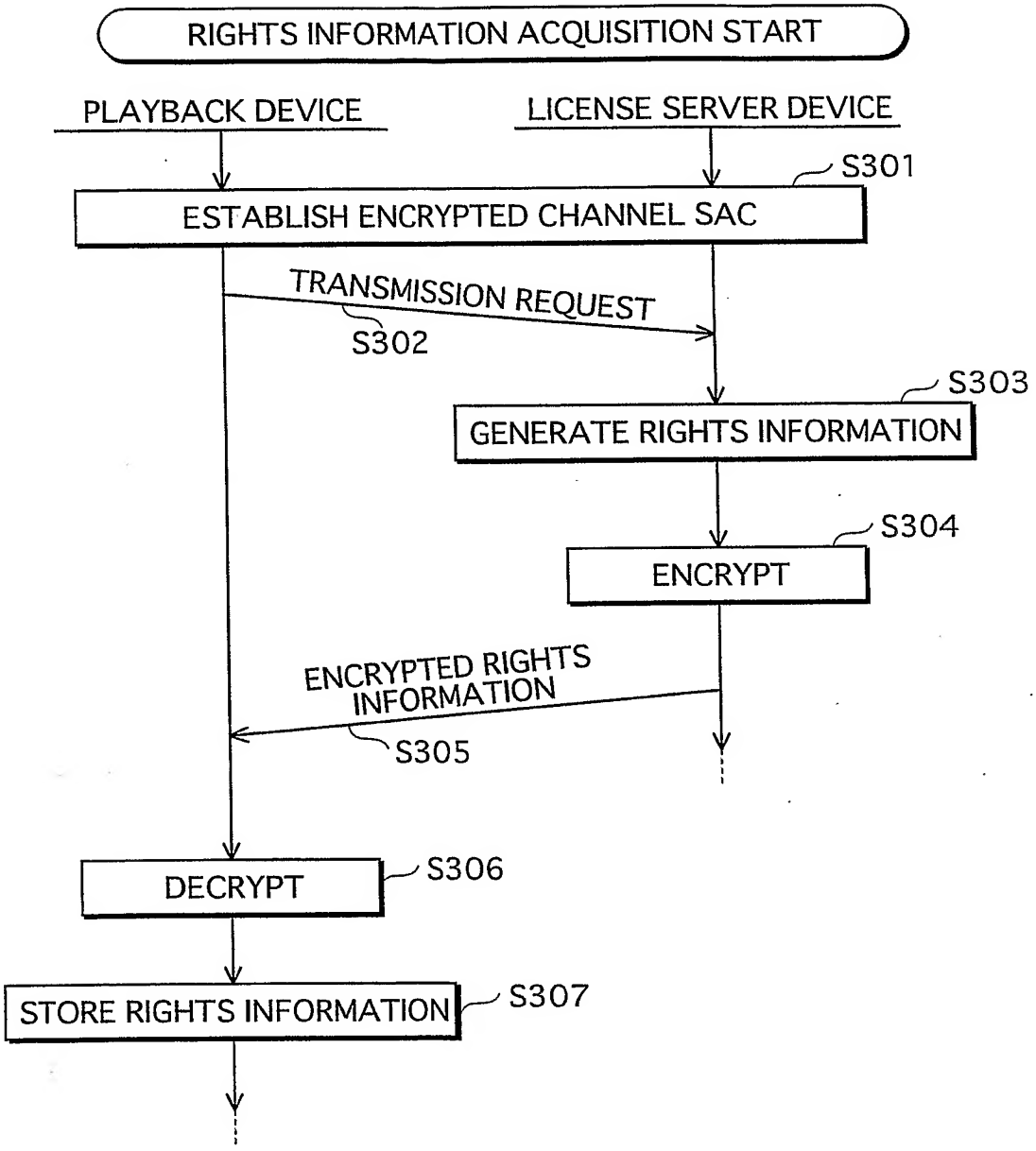
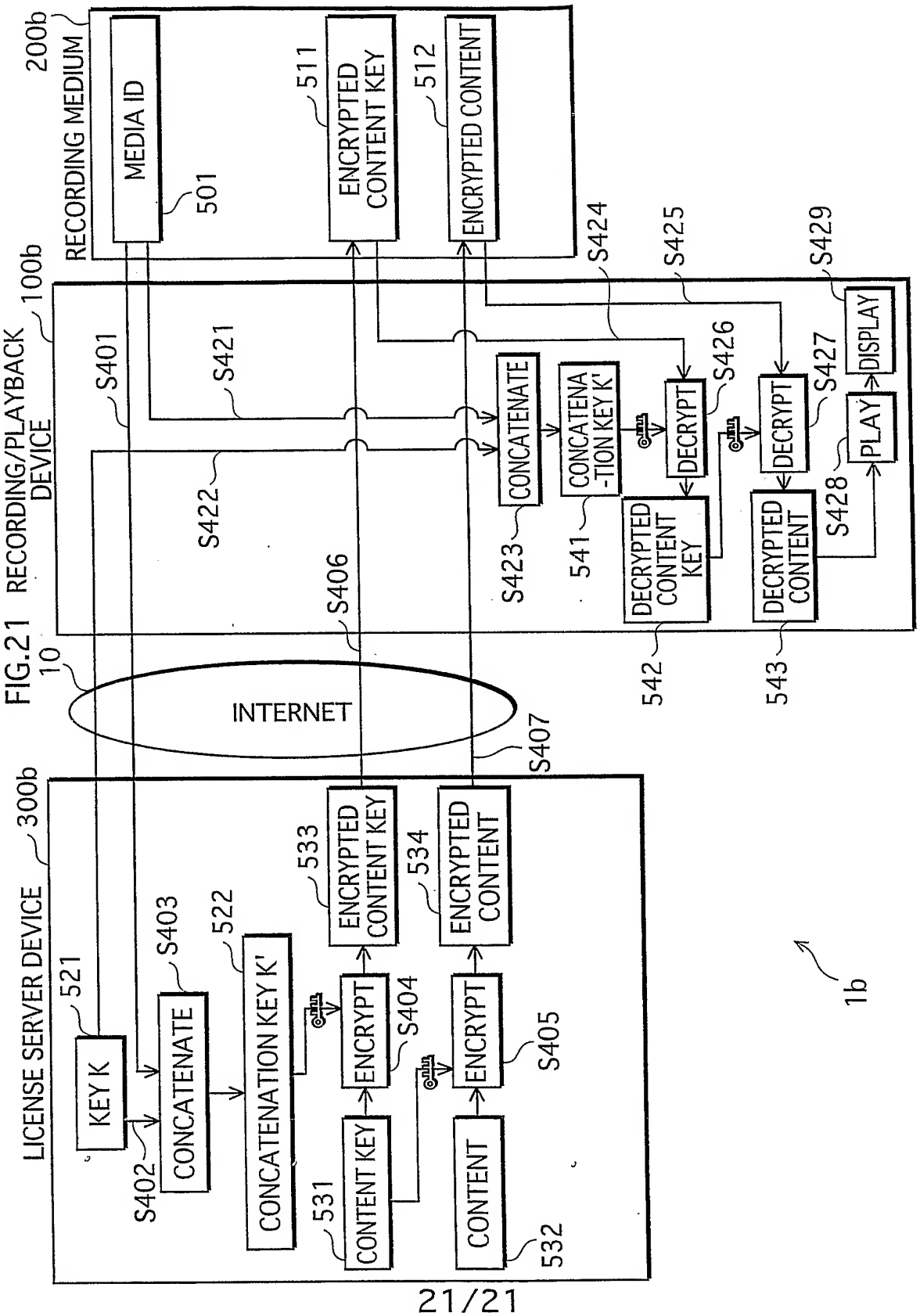

RIGHTS INFORMATION ACQUISITION START
PLAYBACK DEVICE
LICENSE SERVER DEVICE
S301
ESTABLISH ENCRYPTED CHANNEL SAC
TRANSMISSION REQUEST
S302
S303
GENERATE RIGHTS INFORMATION
S304
ENCRYPT
ENCRYPTED RIGHTS INFORMATION
S305
DECRYPT
S306
STORE RIGHTS INFORMATION
S307

FIG.21


200b
RECORDING MEDIUM
MEDIA ID
501
511
ENCRYPTED CONTENT KEY
512
ENCRYPTED CONTENT
100b
RECORDING/PLAYBACK DEVICE
S401
S421
S422
S406
S423
CONCATENATE
541
CONCATENA -TION KEY K'
DECRYPTED CONTENT KEY
542
DECRYPT
S426
S424
S425
S429
DECRYPT
S427
DISPLAY
PLAY
S428
DECRYPTED CONTENT
543
10
INTERNET
S407
300b
LICENSE SERVER DEVICE
KEY K
521
S402
CONCATENATE
S403
522
CONCATENATION KEY K'
531
CONTENT KEY
ENCRYPT
S404
533
ENCRYPTED CONTENT KEY
ENCRYPT
S405
534
ENCRYPTED CONTENT
CONTENT
532
1b